Section:	06	Title:	Information Security
Sub Section:	03	Title:	Information Security
Document:	02	Title:	Application Security

1. STANDARD

To achieve application and information integrity and confidentiality, adequate safeguards will be incorporated into all application’s life cycle.

1.1. Summary of Standard Changes

1.2. Purpose

To develop standards and procedures to insure that proper security elements are incorporated into all software from inception through all changes or modifications throughout the software’s life cycle.

1.3. Scope

Applies to all software used by ISD in its daily business.

1.4. Responsibilities

1.5. Definitions and Abbreviations

1.6. Description of Standard

This standard will control the development, change, and monitoring processes for ISD software as it relates to protections within a secure environment.

1.7. Implications

There will be security controls identified as standard for all software used by ISD. Prior to development or purchase these control elements will be identified and incorporated into ISD software. Software will be developed according to established conventions with formal specifications required, testing completed in a sanitized environment, full documentation required, and all unauthorized access paths removed before production status is granted. There will be a formal change control procedure including separation between production and development environments, restrictions on development staff having access to production information, testing procedures, and documentation standards. Monitoring and diagnostic testing will be restricted to authorized personnel.

1.8. References

1.9. Attachments

2. APPLICATION PURCHASE AND DEVELOPMENT CYCLE PROCEDURES

During the application purchase and/or development cycle, formal specification will be developed, standard conventions followed, ‘sanitized’ testing procedures followed, full documentation created, and at completion, all special access paths removed.

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. Prior to software purchase or development, written, formal specifications are developed by the information owners, software development project manager, and Security Manager specifying functionality, and clearly defining security requirements to be incorporated into the software. The specifications are completed and signed by all parties before purchase activities and/or development begins.

2.2.2. Formal documentation is created and approved by all parties prior to development detailing functionality and security procedures. The documentation is written so that it can be used by persons unacquainted with the processes.

2.2.3. The project manager monitors the creation of the software confirming that development subscribes to ISD standards, procedures, and other system development conventions as established in the EAS guidelines.

2.2.4. Unless prior written permission is obtained by the information owner, testing is performed using ‘sanitized’ production information with no specific details that might be valuable, critical, or sensitive.

2.2.5. Prior to placing the software in production status, all special access paths will be removed so that access may only be obtained via normal secured channels.

2.3. References

Refer to EAS Guidelines

2.4. Attachments

3. SOFTWARE CHANGE CONTROL PROCEDURES

A formal change control procedure, pursuant to EAS change control policy, is used for all system changes assuring that only authorized changes are made at approved times and in approved manners.

3.1. Summary of Procedure Changes

3.2. Procedure Details

3.2.1. Prior to changes, project parameters, using EAS change control standards, are approved in writing by the information owner, production staff, and security where applicable.

3.2.2. Development is kept strictly separate from production environments by the use of no less that separate directories/libraries with strictly enforced access controls approved by security complying with owner requirements.

3.2.3. The application staff does not access or use production information during development unless such information is relevant to the particular application software.

3.2.4. Formal testing for day-to-day operation is conducted by those other than the production staff and monitored by the information owner and security where applicable.

3.2.5. Documentation reflecting all significant changes to production systems notating proposed changes, all approvals, and the way in which changes were performed is completed before completion of the project.

3.3. References

EAS Change Control Standards

3.4. Attachments

4. SOFTWARE MONITORING AND TESTING PROCEDURES

Access to system utilities used to test/monitor or correct system problems are restricted to a small number of trusted employees.

4.1. Summary of Procedure Changes

4.2. Procedure Details

4.2.1. Utilities which can be used to override either system or application access controls such as database troubleshooting tools and disk repair utilities are only used by authorized personnel.

4.2.2. When these utilities are excited, resulting activity is securely logged and promptly reviewed by the computer operations manager or their designee.

4.2.3. A list of personnel authorized to access such utilities is provided to security and only those personnel are give access to the utilities.

4.3. References

4.4. Attachments